ENABLING SSH PROTOCOL VISIBILITY IN FLOW MONITORING

Wednesday 10th April, 2019

Pavel ČELEDA
Petr VELAN, Benjamin KRÁL
Ondřej KOZÁK

CSIRT-MU

Introduction

SSH – Secure Shell

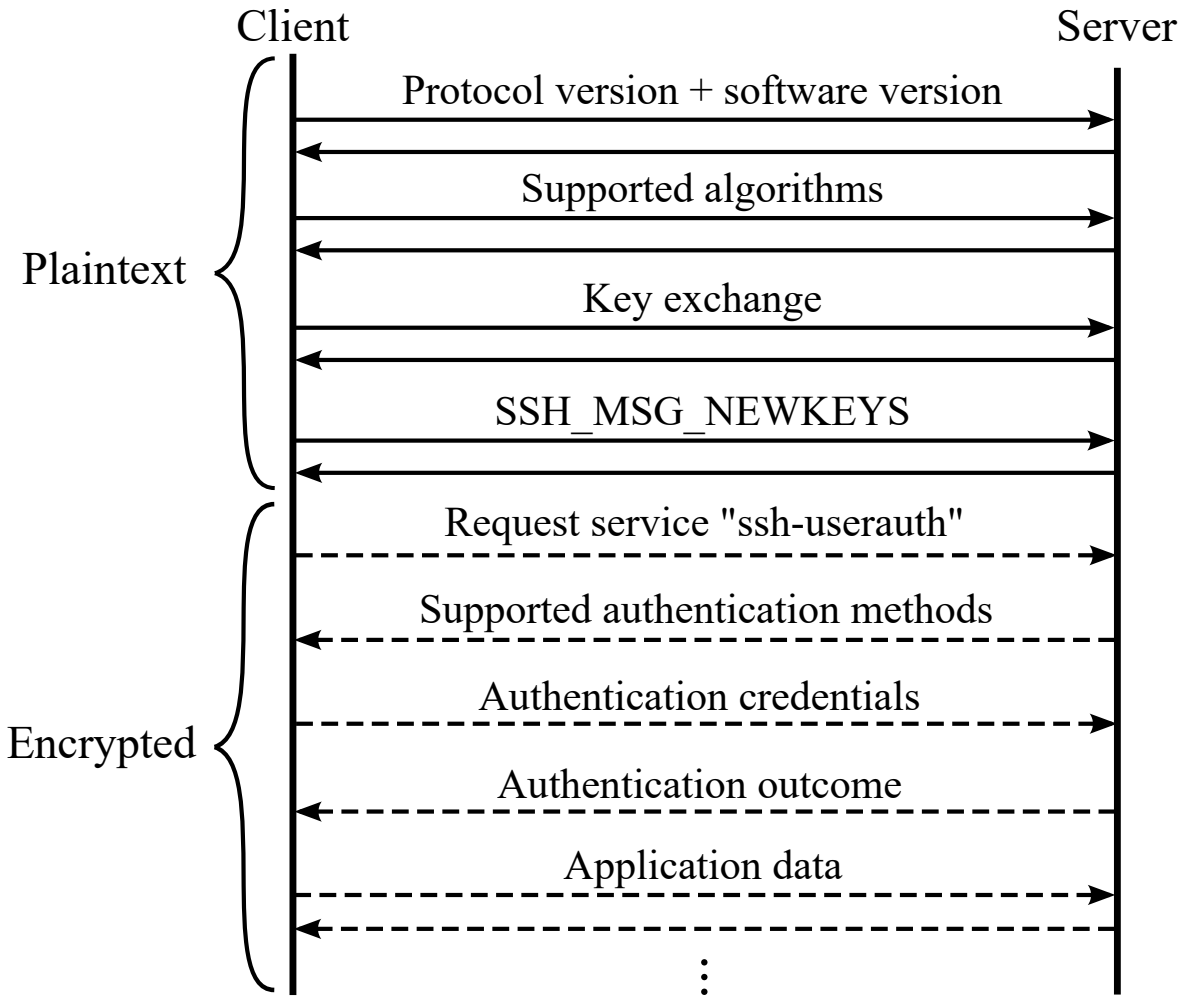
- provides secure connection over an unsecured network
- remote command-line login and remote command execution
- target of network scans, brute-force and dictionary attacks

Research Goals

- propose flow-based (IPFIX) application level SSH visibility
- analysis of SSH traffic – operational relevant use-cases
- provide anonymized dataset used for the evaluation

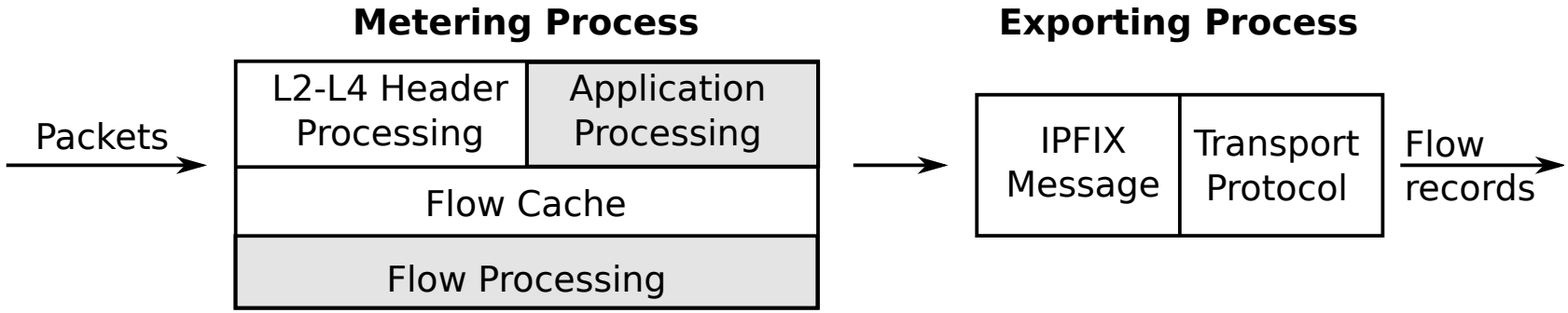
SSH Protocol Measurement

SSH Connection Setup



CSIRT-MU

SSH-Aware Flow Monitoring



Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Packets	Bytes
14:33:12.329	0.648	TCP	147.251.165.135:47466	147.228.240.28:22	.AP.SF	219	275100
14:33:12.334	0.643	TCP	147.228.240.28:22	147.251.165.135:47466	.AP.SF	43	6439

Application	Version	Client Application	Server Application	Key Exchange Algorithm
SSH	2.0	OpenSSH_7.4p1 Debian-10	OpenSSH_6.7p1 Debian-5	ecdsa-sha2-nistp256

Client Encryption	Server Encryption	Compression	Login Attempts
chacha20-poly1305	chacha20-poly1305	none	1

CSIRT-MU

SSH-Aware Telemetry

SSH-Aware Telemetry

SSH Visibility

- passive flow monitoring – Flowmon probe, IPFIXcol collector
- SSH protocol detection (aka Cisco NBAR2) – any port
- client/server SSH information – IPFIX information elements

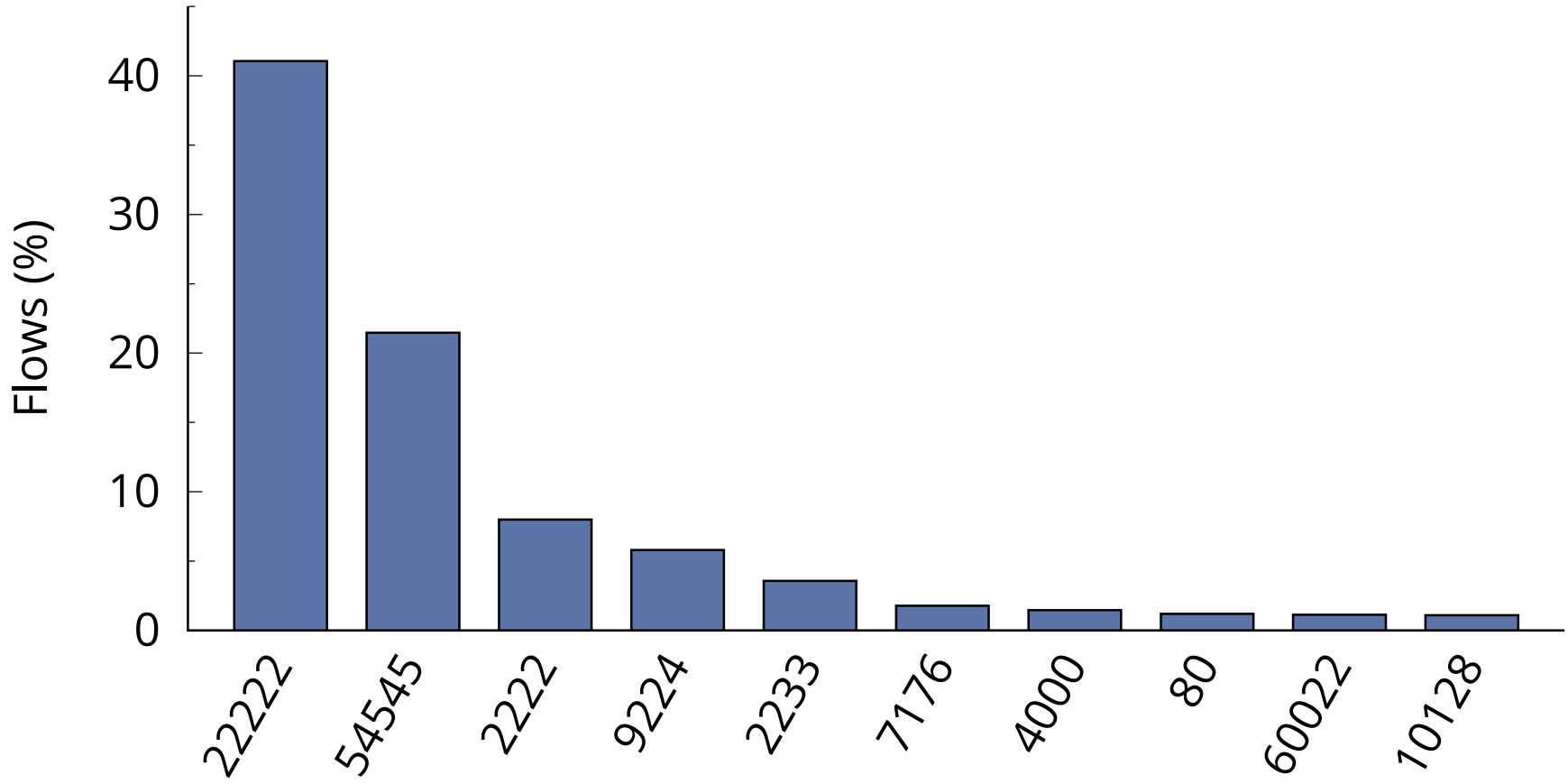
Test Setup

- developed Flowmon probe plugin to provide SSH information
- deployed at the perimeter of the campus network of the MU

Many Operational Relevant Use-Cases

- SSH is widely used by developers, admins, and attackers
- we need to understand our SSH traffic (campus wide)

Top 10 Non-Standard SSH Ports



CSIRT-MU

SSH Software Implementations

Client Software	% of Flows
OpenSSH	37.935
libssh2	23.289
check_ssh	18.107
libssh	10.016
PuTTY	2.510
Go	2.196
paramiko	2.171
WinSCP	1.022
zabbix_agent	0.741
Granados	0.331
nsssh2	0.057
FileZilla	0.007

Server Software	% of Flows
OpenSSH	91.827
Cisco	1.680
libssh	0.238
dropbear	0.243
HomeSSH	0.020
ROSSSH	0.033
conker	0.032
mod_sftp	0.004
FlowSsh	0.012
Zyxel	0.001
Comware	0.003
CerberusFTPServer	0.000

SSH Scanning
and
Brute Force Attacks

SSH Scanning and Brute Force Attacks

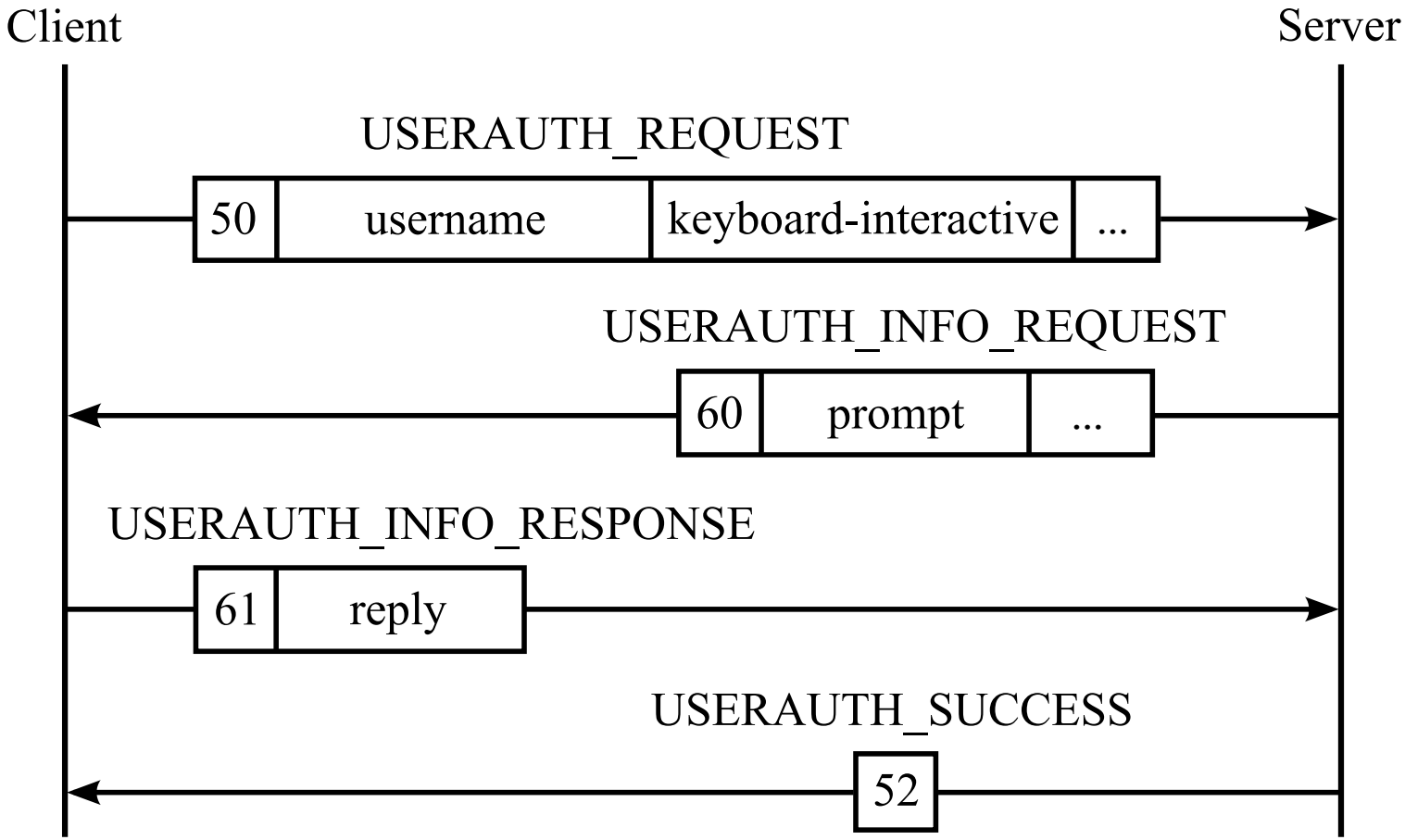
SSH Remote Login Attacks

- attempts to access computer systems by remote attackers
- scanning IP address(es) – looking for systems running SSH
- brute-force attacks – guessing usernames and passwords

Attackers vs. Researchers

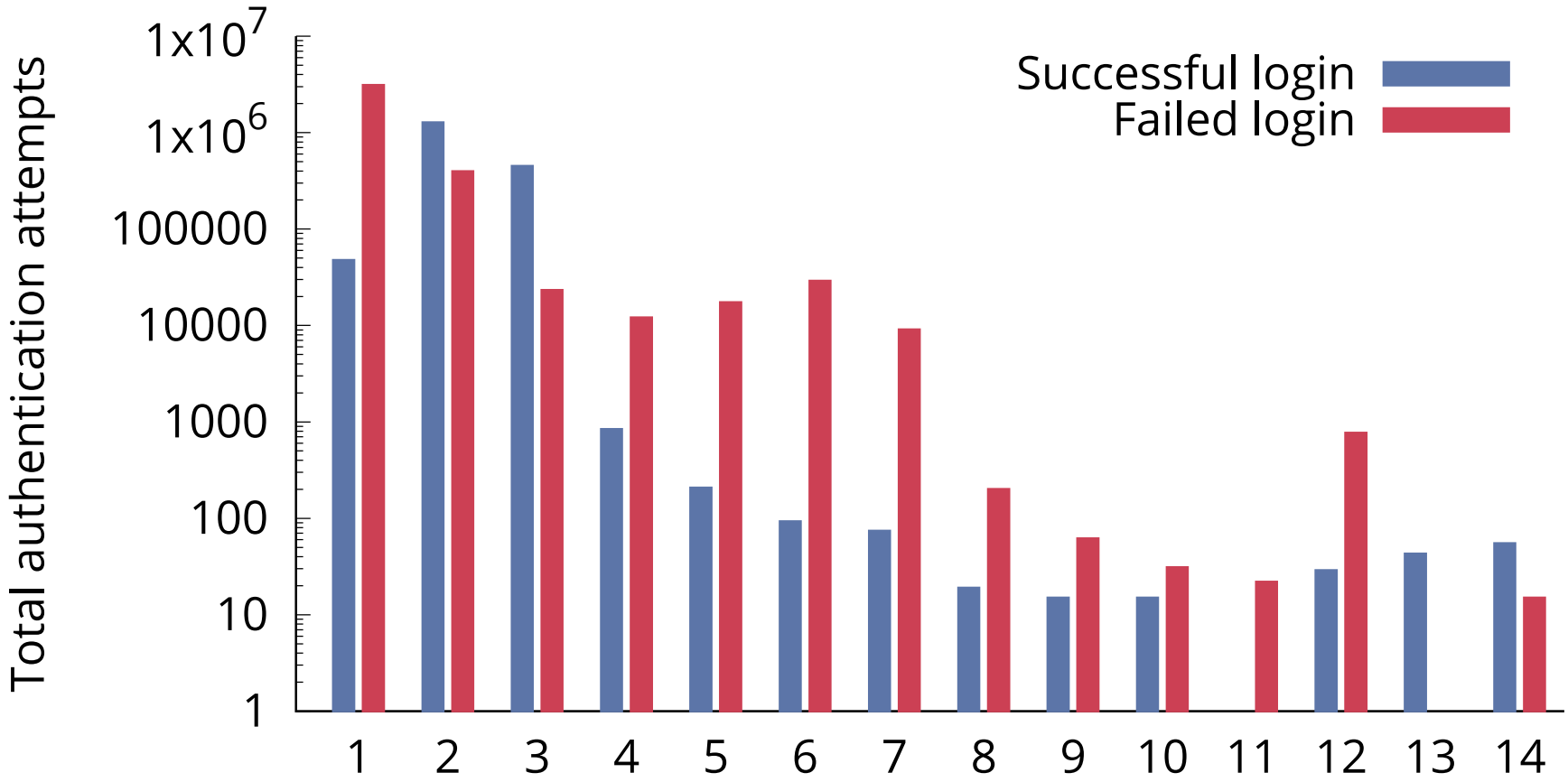
- many attempts to detect scanning and brute-force activities
- high number of SSH scans – no added value in detection
- we need to detect successful logins – utmost importance

User Authentication – Keyboard-Inter. Method



CSIRT-MU

Authentication Attempts per SSH Connection



CSIRT-MU

Unsuccessful SSH Clients

Client Software	% of Flows
libssh2	39.746
check_ssh	34.909
libssh	17.847
OpenSSH	3.001
Go	1.603
zabbix_agent	1.429
Terminal	0.413
Granados	0.366
paramiko	0.340
PuTTY	0.077
WinSCP	0.017

Conclusion

Conclusion

SSH Traffic Analysis – Lessons Learned

- SSH measurement may be tricky (e.g., persistent connections)
- SSH bad practise – non-standard ports, password logins
- threat landscape evolves very fast – scans vs logins
- it is possible to detect (in most cases) successful / failed logins

Future Work

- SSH client / server fingerprinting, and clustering
- identification of SSH communication patterns in the clusters

SSH Dataset Description

Basic Flow Elements

Flow Start Timestamp
Flow End Timestamp
Source IP address (Anon.)
Source Transport Port
Destination IP Address (Anon.)
Destination Transport Port
Transport Protocol
Number of Packets
Number of Bytes
TCP Flags

SSH Elements

SSH Client / Server Version
SSH Client Application
SSH Key Exchange Algorithm
SSH Host Key
SSH Client / Server Encryption Alg.
SSH Client / Server MAC Alg.
SSH Server MAC Alg.
SSH Client Compression Alg.
SSH Server Compression Alg.
No. of Authentication Attempts
Authentication Attempts Result

Dataset available for download
http://dx.doi.org/10.5281/zenodo.1412596

CSIRT-MU

THANK YOU FOR YOUR ATTENTION

csirt.muni.cz

@csirtmu

Pavel ČELEDA

celeda@ics.muni.cz

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

CSIRT-MU